

INTELLIGENCE CHALLENGES AT THE EUROPEAN UNION LEVEL

Colonel Robert CĂLINOIU, PhD Student

EU Military Staff

Colonel (r.) Prof. Dănuț-Mircea CHIRIAC, PhD

“Carol I” National Defence University, Bucharest

Since its creation in 1950, as an organisation of states sharing primarily economic interests, the European Union (EU) has been developed continuously on multiple levels, the security and defence domain being one of the most dynamic starting in 2000. Therefore, in 2001, there were established the Political and Security Committee – PSC, the EU Military Committee – EUMC, and the EU Military Staff – EUMS – within the General Secretariat of the EU Council. Eventually, after the creation of the European External Action Service (EEAS) in 2009, EUMS has changed the subordination to this structure.

One of the five directorates of EUMS is the Intelligence Directorate – DINT whose mission is to provide strategic intelligence to its customers.

Along the process of developing and improving the intelligence activity, in 2007 the EEAS leadership made the decision of creating the Single Intelligence Analysis Capacity – SIAC, bringing together the military expertise of DINT and the civilian intelligence knowledge of the EU Intelligence Centre (INTCEN).

Since its inception, DINT has proved to be a very effective fusion centre of the national intelligence products, issuing strategic documents of significant interest for the EU and national leaders alike, and positively influencing the EU and member nation’s security. Nevertheless, the importance of a flawless functioning of DINT and SIAC results not only from its successes but also from failures, which could have had a major impact on the security of some European states or at the EU level. One of this is the shot down of the Malaysia Airlines Flight 17 (MH17) over the Ukrainian airspace, whose case study we will present in the present article.

Keywords: security; defence; European Union; military/civilian defence information; strategy;

INTRODUCTION. SHORT HISTORY OF THE ESTABLISHMENT OF THE DEFENCE STRUCTURES WITHIN THE EUROPEAN UNION

The European cooperation initiatives in political and economic domains have their origins after the end of the Second World War. After discussions in bilateral and multilateral formats, in 1948 the Western European Union – (WEU) was created by the Great Britain, France, Belgium, West Germany, Italy, Luxembourg, and the Netherlands. This format permitted consultations on various subjects of common interests, mainly political and economic, but also on European security and defence. The Treaty of Maastricht, becoming one of the cooperation pillars within the European Union, introduced the concept of Common Foreign and Security Policy (CFSP) starting 1993. The Treaty affirmed that *“the common foreign and security policy shall include all questions related to the security of the Union, including the eventual framing of a common defence policy, which might in time lead to a common defence”* (Treaty of Maastricht, Title V, art J 4).

After five years, during the Franco-British St. Malo Summit (4 December 1998), the British Prime-Minister, Tony Blair, and the French President, Jacques Chirac, signed a joint declaration stating that *“the Union must have the capacity for autonomous action, backed up by credible military forces, the means to decide to use them, and a readiness to do so, in order to respond to international crises”* (Joint Declaration issued at the British-French Summit, 1998, Art. 2). The declaration signalled a significant change in the UK stance on security and defence, from blocking any intention of creating military structures within the EU to an open agreement. At the same time, France, that withdrew from NATO’s military structures in 1996 (reversing its position in 2009), was seeking means to consolidate its security within the European Union.

The Joint Declaration allowed the European States to launch, during the European Council in Koln (June 1999), the concept of *European Security and Defence Policy – ESDP*, and at the end of next year, through the Treaty of Nice, to create the legal basis for European cooperation in the field of security and defence by defining the competencies, structures and means necessary to develop a Common Security and Defence Policy (CSDP).

To the creation and development of the formal structures having as tasks the CFSP and CSDP fields contributed, along with the progressive accumulation aforementioned, the security situation in Europe. This had been characterised

by the wars in the Former Republic of Yugoslavia, the disintegration of the Soviet Union and the appearance on its territory of a number of independent states, as well as the increasing number of the terrorist attacks by foreign perpetrators on European soil. The main goal of CSDP has been the management of the crisis outside the EU's territory, objective leading to the creation in 2001 of the following entities: the Political and Security Committee (PSC), the EU Military Committee (EUMC), and the EU Military Staff (EUMS) – within the General Secretariat of the Council.

The EU Council decision stated that, in the field of intelligence, the Military Staff is to perform early warning, situation assessment and strategic planning for missions and tasks referred to in Article 17(2) of the TEU, including those identified in the European Security Strategy.

After the signing of the Lisbon Treaty in 2009 and the establishment of the European External Action Service (EEAS), all CSDP structures, including EUMS, moved from the General Secretariat of the Council to the newly created EEAS. To underline the importance of EUMS as a single source of military expertise within the EU institutions, it was subordinated directly to the High Representative/Vice-President of the European Commission (HR/VP).

SHORT HISTORY OF THE ESTABLISHMENT OF THE INTELLIGENCE STRUCTURES WITHIN THE EUROPEAN UNION

One of the components of the EUMS is the Intelligence Directorate (EUMS Intelligence Directorate – DINT), established in 2001, at the same time as the parent organisation. Its missions include providing intelligence on the political strategic level as well as in support for EU operations and missions, providing a timely and accurate situational awareness and the intelligence input to crisis response planning and assessment for military operations, civilian missions and exercises (EU Council Decision, 2001). The personnel coming from the member states defence intelligence organisations (DIO) as National Seconded Experts (SNEs) for a period not exceeding four years are staffing DINT. Each member state's DIO has a point of contact (POC) within DINT providing the two-way channel of communication and transfer of intelligence products. DINT has no collection means, the classified intelligence coming from the parent DIOs or from the civilian intelligence organisations – CIO (the later via the Intelligence Centre – INTCEN), a civilian structure with whom DINT works closely within the Single Intelligence Analysis Capacity (SIAC) format. A third source of intelligence is the EU Satellite Centre (SATCEN), which is providing products derived from imagery acquired upon request. DINT is also benefiting of information coming from the EU Delegations in various states, gathered by its personnel during

the Fact-Finding Missions (FFM) from Think Tanks or by participating in conferences and seminars having subjects of interest (ongoing or potential crises areas). The inputs from DIOs or CIOs are submitted on a voluntary basis, having subjects connected with areas or topics of immediate interests for a certain member state (crisis, terrorism, illegal migration etc.) (Ibid., p. 6, point a).

The Production Branch is organised in geographical and subjects sections (transnational and hybrid threats). Its products are delivered in written format or oral briefs, planned or upon EU leaders' request. Among the issued documents, there are Intelligence Briefing Notes, Threat Assessments, and Intelligence Assessments. Periodical issued intelligence products are Annual Global Threat Review – AGTR, and SIAC Weekly.

The management of the intelligence domain is performed, from the member states' DIOs perspective by the Board of Directors (BoD), composed by the directors of the military intelligence services from EU member states. BoD convenes once a year, or as many times as situation requires. In order to prepare the BoD meeting, two other working groups take place, at the Directors for Analysis and the Plans and Policy Directors.

On the civilian side, in 1999, it was created the Joint Situation Centre (SITCEN, having the mission to produce open source analysis (OSINT). In 2002, SITCEN becomes a forum of exchanging classified information between itself and seven EU member states (France, Germany, Italy, The Netherlands, Spain, Sweden, and Great Britain).

SITCEN grew progressively by accepting more member states' civilian intelligence organisations, eventually becoming (2012) the Intelligence and Analysis Centre (INTCEN), a civilian intelligence organisation at the level of the general directorate within EEAS, under the direct subordination of HR/VP, and the main DINT partner within the SIAC format.

INTCEN has two main divisions, the Intelligence Analysis Division and the Open Source Research and Support (OSINT) Division (Impetus, 2019, p. 10).

The Intelligence Analysis Division covers both the regions of major interest for the EU CFSP/CSDP according to the 2016 EU Global Strategy, and the subjects of concern for EU' security like counterterrorism, non-proliferation, migration, energy security, cyber and hybrid threats. Unlike DINT, INTCEN benefits by EU carrier employees, beside the National Seconded Experts coming from the CIOs of the member states.

In order to better inform the leadership on the growing hybrid threats directed at the EU, in 2016, DINT and INTCEN created the Hybrid Fusion Cell, with experts from the two structures. The Hybrid Fusion Cell analyses matters like disinformation, cyber-attacks, psychological operations (psyops), subversive actions, terrorism,

sabotage, exploitation of the cultural, language or religious divisions, illegal economic activities directed to attain political advantages (*“pipeline politics”*), support for secessionist movements, migration and migrants exploitation, use of mercenaries and third parties in covert actions (Barber et al.).

EU Satellite Centre (SATCEN) is also an important part of the intelligence architecture of the European Union. Established in 1993 under the name of Western European Union Satellite Centre, it has functioned under the current designation since 2002. Operationally coordinated by the EEAS, SATCEN provides early warning of potential crises and imagery products on the customer’s request, the main beneficiaries being DINT and INTCEN. Other EU organisations, like EUROPOL, FRONTEX, Civilian Planning and Conduct Capability (CPCC) are among its customers, as well as the EU member states. Its products are based on the exploitation of spatial and aerial capabilities (GEOINT and IMINT), corroborated with collateral data from OSINT or Social Media Intelligence (SOCMINT) (Salmi).

EU INTELLIGENCE SUPPORT ARCHITECTURE AND THE WORKING RELATIONSHIPS OF ITS INTELLIGENCE STRUCTURES

In 2012, after the establishment of the EEAS and taking into account the growing threats of the security environment, the HR/VP issued the decision of founding the EEAS Intelligence Support Architecture – ISA (Impetus, Ibid., pp. 10-11).

The main goal of ISA has been to take into account all relevant developments and design an intelligence support package – to define responsibilities, provide direction and guidance, and create provisions for effective production and fast, secure and reliable dissemination of intelligence products to the EU decision-makers and member states. The ISA also includes provisions on coordination and liaison with the MS intelligence organisations, European Commission and with international organisations.

The above-mentioned HR/VP Decision defines *“intelligence”* as information that has been collected, processed and disseminated for the use by decision-makers and other customers and ISA as structures, processes and activities related to intelligence. It aims to optimise the intelligence function within the EEAS and encourages close cooperation and coordination across EU institutions and between intelligence stakeholders.

ISA included in 2012 two central structures – the Intelligence Steering Board (ISB), transformed in 2019 by a new decision issued by the HR/VP, Josep Borrell, Intelligence Policy Board (IPB), and Intelligence Working Group (IWG). EU INTCEN and DINT provide jointly the Secretariat function for both ISB and IWG. The ISB

defines intelligence requirements and priorities at the strategic level as well as endorses structural, organisational and policy measures required to improve the Architecture. It also provides guidance to address deficiencies in the field of security. The HR/VP or EEAS Executive Secretary General (ESG) chairs the Board.

The IWG further defines, specifies and adjusts EEAS intelligence requirements and priorities. In particular, it proposes the strategic intelligence direction and Prioritised Intelligence Requirements (PIR) for the intelligence. The IWG synchronises the tasking of the Single Intelligence Analysis Capacity (SIAC), defines SIAC product range, develops and monitors a feedback mechanism. The IWG is co-chaired by the Director EU INTCEN and Director EUMS INT.

The establishment of the Single Intelligence Analysis Capacity – SIAC was possible due to the development by the former Secretary General/High Representative (SG/HR) Javier Solana of the concept of Comprehensive Approach to the external crises and conflicts.

The idea at that time was to bring together, in a functional way, analytical capacities from both the EU Situation Centre (EU SITCEN, now renamed EUINTCEN) and DINT, thus benefiting from a wide EU knowledge base for producing enhanced and reliable intelligence. This resulted in the SIAC arrangement initiated by directors of EUMS and EU SITCEN at the beginning of 2007. In addition, and in line with the Comprehensive Approach concept, the EU intelligence community intensified its efforts to widen the scope of access to and utilisation of all the information and data already available within the EU.

SIAC has become one of the EU forerunners in the field of producing synergies by a joint civilian-military approach, providing high valuable intelligence to the EU and member states. The creation of EEAS and the transfer of EUMS and INTCEN to it has led to a significant increase of demand for specific products and, accordingly, the tasks multiplied.

In the SIAC format is taking place the sharing of intelligence received from DIOs and CIOs through the secured national channels, the PIR issued by IPB are detailed and answered, joint task forces mixing the military and civilian intelligence expertise are created to tackle various subjects of interest. One of the successful examples is the Hybrid Fusion Cell, created to analyse the specific threats directed against the EU interests and providing intelligence in this new field of security.

SIAC intelligence products are disseminated to EU decision-makers and DIOs and CIOs of the member states, from this viewpoint SIAC working as an Intelligence Fusion Centre. The advantage of this format resides in the sharing of expertise from one member state to another on subjects of temporary interest (new crises, mission preparation, specific training).

In addition, SIAC organises working groups where experienced analysts from CIOs, DIOs, international partners (NATO) or Non-Governmental Organisations (NGO) participate and share their knowledge on different topics of interests in common benefit of participants. Moreover, within SIAC there are formed joint teams for Fact Finding Missions (FFM) in areas of concern.

To meet all these challenges, further systemic transformation is needed. At this stage, it is essential to revise and optimise processes, change the information sharing intelligence culture within the EU, adopt suitable technology and adjust the conceptual approach to the intelligence support function. In short, promote intelligence within the EU, as well as produce intelligence for the EEAS with a more operational and dynamic approach.

INTELLIGENCE CULTURE WITHIN THE EU – MAJOR VULNERABILITY IN COUNTERING THE THREATS AND DIMINISHING THE RISKS

The culture particular to the intelligence domain at the European level is in its early stages of development due to a series of factors. First, it is the continuing transformation of the EU, now comprising of 28 members after reaching its peak of 27, each having its own interests, identities, similar but not identical security cultures. Equally important, the defence and security domains are in the national responsibility (Treaty on European Union and Treaty on the Functioning of the European Union, Title I, Art. 4, Para. 2), the European policies in this fields having to harmonise diverse interests and particular approaches. The decisions in the security and defence fields have to be taken by consensus. Member states' policies are usually based on the national intelligence inputs, grounded on information acquired proportionally with the resources available, internal priorities (focus on crisis in their proximity) and thus incomplete or biased.

The consequences of this reality at the EU level are difficult mediation of interests, unnecessary multiplication of efforts (financial or human) for the same identified threat (e.g. illegal migration or terrorism) or the lack of a common strategy to counter transnational threats.

Not least, a major impediment in the development of a European intelligence culture is the lack of appetite of the member states to create common independent intelligence structures having all the necessary means for collecting, processing and delivering relevant intelligence products to all customers, EU institutions or member states. The lack of solid EU intelligence structures efficiently working in the benefit of EU's security and defence, and becoming renown over time, has a major impact in maintaining the current culture where the written classified information generates more administrative concerns than benefit on subjects of strategic interest.

The lack of timely information and the slow adaptation of the structures to the current challenges represent also aspects that should be addressed in order to increase the profile of the intelligence within the EU. The illegal migration and its associated facets (terrorism, organised crime), which caused a major threat to the security of the EU and a long debate among the member states, was perceived very late as a threat of a strategic level. The cyber threats promoted by entities difficult to detect are also countered with insufficient means at the EU level, the centre of gravity resting on the nations, while the modus operandi is by definition international.

Using proxies in a foreign country for attaining military, political, and economic goals is a strategy more and more used and causing difficulties in being countered by the democratic states and organisations using the existing legal means. While the sponsors are easy to detect, the lack of instruments to counter this strategy leads to protracting conflict and crises generating regional instability and security challenges to EU. Without a proper security, the criminals are using the fundamental rights like the freedom of movement to challenge the EU's security and its citizens wellbeing. The terrorist attacks in Madrid, Paris, and Brussels are the most notorious examples of this kind. The cyber-attacks or phishing attempts against EU institutions request a decisive riposte from a solid defence system.

Changing by force the borders of states thus affecting the security in the EU's proximity (Crimea), influencing the free and democratic elections by third parties using illegal means, manipulating the national referendums having a direct and significant impact on EU's existence (BREXIT), disinformation campaigns in EU member states concerning the EU's institutions policies and actions, encouraging the secessionist movements and radicalism are examples requiring strong EU intelligence institutions capable of providing early warning, detecting and timely countering such actions.

Finally, yet importantly, a well-timed and adequate reaction to a military crisis in the close neighbourhood of the EU could raise the awareness of the population and avoid dramatic consequences to the security of the Union and its citizens. Such an example will be analysed in the case study below.

CASE STUDY ON THE SHOT DOWN OF THE MALAYSIA AIRLINES FLIGHT MH17 (MH17) OVER THE UKRAINIAN AIR SPACE. LESSONS LEARNED

Case studies concerning successful operations or major failures with strategic impact have been, throughout history, a preoccupation for the professionals demotivated by the chain of command (Plame, 2007, p. 8), academics looking for improving the field (Ibid.), or visionary leaders wanting to help their successors repeating the same mistakes (Bush Jr., 2010, Powell, 2003, Rice, 2011).

In analysing the failures, two main situations are described. First, ignoring or diminishing the importance of relevant indicators concerning a possible course of action, which proves in the end to be unfavourable to own interests. The second is the one of a correct and timely analysis presented by the intelligence services to the decision-maker, without being capable of convincing the later to act accordingly and avert the negative consequences (Wirtz).

The necessity to study the intelligence failures and extract useful lessons goes back in the past and is always a requirement in order to avoid repeating the same mistakes. Nowadays, when the technology allows the fast access to knowledge and rapid exchange of information and it is more and more difficult for one state to attribute hybrid or asymmetric actions to a certain entity without cooperating with a wide array of other organisations, learning from mistakes is essential. Analysing the techniques, tactics and procedures in the cases of killing of political opponents on the soil of EU states, meddling in the elections of foreign states perceived as enemies, cyber-attacks of critical infrastructure for intimidation or economic advantages is mandatory in order to defend the security of a nation or alliance. Studying the favourable conditions leading to this kind of attacks, like prolonging the stay in power of authoritarian leaders with expansionist visions in pseudo-democratic states and dismissing the international rule of law in favour of the rule of the most powerful may provide the right tools and measures against the villains. Difficult to attribute, the asymmetric attacks escape from the classical definition of an armed aggression of the UN Charter¹ and the eventual tailored, lawful international punishment following a resolution in the UN Security Council. The failure in taking adequate measures, other than weak economic sanctions against persons and countries, or blaming them at international conferences encourages the perpetrators to repeat the deeds. In these circumstances, it is even more demanding for the intelligence services to perform early warning, counter such hostile actions and this could be done only by analysing and offering efficient solutions to the current challenges.

The events

The crisis in Ukraine erupted on 21 November 2013, when Ukrainian citizens starting protesting in the capital city of Kiev against the President Victor Yanukovich following his decision to reject a project for a greater economic European integration

¹ Article 51, UN Charter, states: *“Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security”.*

of Ukraine. The protesters gathered in the Independence Square being met with force by the regime, which led to a rapid increase of their number. Determined in expressing their demands, the demonstrators soon renamed the Independence Square as Euromaidan (European Square).

The protest progressively escalated, eventually leading to an armed confrontation. In the timeframe of 18 to 20 February 2014 the battle between the camps resulted in approximately 130 deaths, among which 18 were members of the security forces. Being clear that a national reconciliation was not possible without an international involvement, the EU and the Russian Federation helped reaching an Agreement, signed on 21 February 2014 (Kariakina et al.). However, for unknown reasons, the Russian Federation representative refused to sign the document at the last moment. The failure of mediation and the violent escalation of the conflict led to the ousting of the president Victor Yanukovich and the takeover of power by a heterogeneous group of people.

Taking advantage of the crisis developments and the power vacuum, in March 2014, the Russian Federation troops stationed in Crimean Peninsula due to a bilateral agreement between the two countries (Partition Treaty), and special forces troops without identification badges, deployed earlier, started taking over progressively the Ukrainian bases and the Crimean Peninsula territory.

In order to politically formalise the hostile takeover, in the occupied territory it was organised a referendum on which the citizens had to choose Crimea's integration within the Russian Federation or the return to the provision of the 1992 Constitution and being part of Ukraine. The results of the referendum (contested at the international level) showed the supposed will of the majority of the population (96.77% of the votes from an 83.1% turnover) to become a part of the Russian Federation (Russia Today, 2014).

Subsequently, motivating that the rights of the Russian citizens and Ukrainians of Russian origins had to be protected in South-Eastern Ukraine, secessionist movements from Donetsk and Luhansk regions organised similar referendums, declaring the Popular Republics on both regions.

The statements of independence of separatists in the two aforementioned regions led to transforming the ethnic divergences in armed conflicts between the Ukrainian security forces and the local paramilitary backed by covert Russians military capabilities (Anders Fogh Rasmussen, Speeches & Transcripts, 2014). On this overall dissolution of the state authority, combined with classical war tactics, psychological warfare, and hybrid actions, the shot down of the Malaysia Airlines Flight MH17 (MH17) over the Ukrainian air space (Hrabove) took place.

MH 17 took off from Amsterdam to Kuala Lumpur on 17 July 2014. The flight route of the planes from Amsterdam to Kuala Lumpur routinely passed over the Ukrainian territory, precisely over the Donetsk region where an armed conflict involving high calibre armament, including ground to air artillery was used. Even though there was information that artillery systems capable of shooting down an airplane flying over 10,000 meters² were in the hands of the separatist forces, either sized from the warehouses of the Ukrainian Armed Forces or received from friendly entities, the flight restrictions (Notice to Airmen – NOTAM) in place concerned only flights below 9,700 meters, and not the complete interdiction of flights over the war zone. Indeed, various media reports³ indicated in June that a missile launcher system BUK-M1 has been sized and repaired by the separatists⁴, while the transfer of different military capabilities by the Russian Federation over the border in the secessionist regions was common knowledge.

At approximately 15.20 (Central European Time – CET) MH 17 disappeared from radars in the Hrabove area and the communication of the Ukrainian Air Traffic Service with the plane had been lost. Even though it was not clear immediately what happened, separatists radio communications indicated their belief that they succeeded in shooting down a military Ukrainian plane AN-26⁵. Four days after the crash, the United Nations Security Council unanimously adopted Resolution 2166, expressing support for an independent international aviation investigation into the crash.

The official report that followed, issued by the Dutch Safety Board⁶, arrived to the conclusion that the in-flight disintegration of the plane near the Ukrainian/Russian border was the result of the detonation of a warhead. The weapon used was a 9N314M – model warhead carried on the 9M38-series of missiles, as installed on the Buk surface-to-air missile system.

It is worth mentioning that, in one week before the crash of the MH 17, 888 flights passed over the same territory facing the same security risks, unidentified by any national and international entity, military or civilian.

² According to the official data, the Boeing 777 was flying at an altitude of 10,100 meters; <https://libraryonline.erau.edu/online-full-text/ntsb/miscellaneous-reports/mh17-crash-en.pdf>, retrieved on 18 October 2020.

³ On 6 June 2014, *The International New York Time*.

⁴ On 11 June 2014, *Argumenty nedeli*.

⁵ On 14 June 2014 the separatists shot down an IL-76 airplane belonging to the Ukrainian Air Forces, while landing at the Luhansk International Airport, causing the death of 49 soldiers; on 14 July 2014 the separatists shot down an AN-26 airplane belonging to the same Ukrainian Air Forces flying at an altitude of 6,500 meters, claiming on social media that the success was possible due to the use of a Buk-M1 surface-to-air missile system seized from the Ukrainian Armed Forces and operationalised by own efforts; <https://libraryonline.erau.edu/online-full-text/ntsb/miscellaneous-reports/mh17-crash-en.pdf>, retrieved on 18 October 2020.

⁶ The Dutch Safety Board official reports in English can be accessed at <https://www.onderzoeksraad.nl/en/page/3546/crash-mh17-17-july-2014>, retrieved on 18 October 2020.

Lessons learned

One of the favourable courses of action would have been, from the intelligence services perspective, that through a flawless tradecraft, the mass-media reports concerning the existence in the hands of the separatists of a military capability able to shoot down a plane flying at a high altitude (over 10,000 meters) had been verified via intelligence means, double-checked by military analysts and confirmed or infirmed with a sufficient degree of accuracy thus permitting the eventual transmission of an intelligence product to the decision-makers.

Corroborating the technical data of the surface-to-air systems existent in the area, with the information concerning the recent shooting down of other planes, the constant transfer of military capabilities over the Russian/Ukrainian border, and taking into consideration the asymmetric war characteristics of continuous disinformation, lack of proper training, and the disrespect for the laws of war, a thorough analysis could have reached to the conclusion that the risks posed to the civil aviation are greater than the economic benefits and the comfort of following a known flying pattern.

Another positive course of action would have been the sharing of national pieces of intelligence related to the armed conflict with the European Single Intelligence Analysis Capacity, which could have acted as a fusion centre putting the pieces together and adequately informing the EU institutions and decision-makers, and the EU member states and partners about the security risks. As such, the European Union Aviation Safety Agency (EASA) would have received a useful intelligence product and issued a warning to the European air operators, furtherly informing the International Civil Aviation Organisation (ICAO), which has the duty of issuing NOTAM at the international level.

An additional element, which could have helped avoiding the tragedy, could have been a better cooperation of the Ukrainian security/intelligence institutions with the European counterparts, especially taking into consideration the existence of similar cases even though involving flights at a lower altitude (under 7,000 meters). Closing completely the air space in the conflict area, a national responsibility, would have been a salutary preventive measure, in consensus with the national and international security policies, and more important saving the lives of the 298 citizens from 10 countries.

The failure in preventing the shooting down of the flight MH 17 showed how a regional conflict, insufficiently monitored and analysed, may have major consequences upon the security of the European and international citizens.

Moreover, such an event has the potential of inflaming an existing armed conflict, if among the passengers killed would be citizens with a high political or social profile belonging to states having a high capability of military retaliation and authoritarian leaders in search of global recognition of their power.

The European attentiveness in monitoring the Ukrainian armed conflict and avoiding such tragic situations had to be far greater, as the Ukrainian crisis had started following the strong will of the majority of its citizens for a greater cooperation with the EU – a political, economic, security, and social role model.

BIBLIOGRAPHY:

1. Lt Col Berbel-Lopez, F.R. (EUMS) (2018). CSDP Course presentation, course organised by the European Security and Defence College, in cooperation with the national Defence University, Bucharest.
2. Bush, G.Jr. (2010). *Decision Points*. New York: Crown Publishing Group.
3. Kariakina, A., Sergatskova, K., Kakhidze, A. (2017). *The Maidan Cases in Numbers and in Pictures*, https://en.hromadske.ua/posts/the_maidan_cases, retrieved on 27 September 2020, corroborated with the Amnesty International documents, <https://www.rferl.org/a/ukraine-maidan-justice-victims-amnesty-fifth-anniversary/29779358.html>, retrieved on 27 September 2020.
4. Lassche, D., *Militaire Spectator*, <https://www.militairespectator.nl/thema/internationale-samenwerking/artikel/eu-militarystaff-frog-boiling-water>, retrieved on 12 August 2020.
5. Plame, V. (2007). *Fair Game: My Life as a Spy, My Betrayal by the White House*. New York: Simon and Schuster.
6. Powell, C. (2003). *My American Journey*. New York: Ballantine Books.
7. Rasmussen, A.F. Speeches & transcripts; *Secretary General sets out NATO's position on Russia-Ukraine crisis*, https://www.nato.int/cps/en/natolive/opinions_110643.htm, retrieved on 27 September 2020.
8. Rice, C. (2011). *No Higher Honor: A Memoir of My Years in Washington*. Random House Audio.
9. Salmi, I., former INTCEN Director, interview in *Moondial Nieuws*, Belgium, <https://www.mo.be/en/interview/ilkka-salmi-eu-s-007>, retrieved on 13 September 2020.
10. Wirtz, J.J. (2001). *Intelligence to Please? The Order of Battle Controversy During the Vietnam War*. Political Science Quarterly.
11. EUMS Information Brochure, https://www.cvce.eu/en/obj/information_brochure_on_the_european_union_military_staff_eums-en-1bcbd497-c5e3-4b7a-ab54-9e392e0c1483.html, retrieved on 13 September 2020.
12. Council Decision 2001/80/CFSP on 22.01.2001, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:r00006&from=EN>, retrieved on 13 September 2020.
13. Joint Declaration issued at the British-French Summit Saint-Malo, https://www.cvce.eu/content/publication/2008/3/31/f3cd16fb-fc37-4d52-936f-c8e9bc80f24f/publishable_en.pdf, retrieved on 3 August 2020.

14. Dutch Safety Board Reports, <https://www.onderzoeksraad.nl/en/page/3546/crash-mh17-17-july-2014> and <https://libraryonline.erau.edu/online-full-text/ntsb/miscellaneous-reports/mh17-crash-en.pdf>, retrieved on 23 September 2020.
15. *Impetus* Review, EUMS, no. 17 spring/ summer 2014, http://www.eeas.europa.eu/archives/docs/csdp/structures-instruments-agencies/eu-military-staff/images/impetus_springsummer_14.pdf, retrieved on 3 August 2020.
16. *Idem*, no. 28, autumn/winter, 2019, https://eeas.europa.eu/sites/eeas/files/eums_impetus_28_final_web.pdf, retrieved on 13 September 2020.
17. Official EEAS website, https://eeas.europa.eu/headquarters/headquarters-homepage_en/3602/Organizationchart, retrieved on 23 August 2020.
18. *Treaty on European Union*, Title I, Art. 4, https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_on_european_union_en.pdf, retrieved on 13 September 2020.
19. *Treaty of Maastricht*, Title V – *Provisions on a common Foreign and Security Policy*, https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_on_european_union_en.pdf, retrieved on 13 September 2020.